IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 5:23CR307
	)	
Plaintiff,	)	JUDGE PATRICIA A. GAUGHAN
	)	
v.	)	
	)	
MICHAEL J. ELOSHWAY,	)	GOVERNMENT'S TRIAL BRIEF
	)	
Defendant.	)	

Now comes the United States of America, by and through counsel, Rebecca C. Lutzko, United States Attorney, and Jennifer King, Assistant U. S. Attorney, hereby submitting its trial brief in the above matter in accordance with this Court's Trial Order.

I. CONTROLLING LAW

The Indictment charges Defendant Michael Eloshway ("ELOSHWAY") with one count of Receipt and Distribution of Visual Depictions of Minors Engaged in Sexually Explicit Conduct, 18 U.S.C. § 2252(a)(2) and one count of Possession of Child Pornography, 18 U.S.C. § 2252A(a)(5)(B). The relevant statute for the first offense is Title 18, United States Code, Section 2252(a)(2), which provides:

> "Any person who knowingly receives any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; shall be punished as provided in subsection (b)."

18 U.S.C.§ 2252(a)(2). To sustain its burden of proof for this crime, the United States must prove all of the following elements beyond a reasonable doubt:

1. That the defendant knowingly received or distributed a visual depiction;

2. That such visual depiction was shipped or transported in interstate or foreign commerce by any means, including by computer;

3. That the production of such visual depiction involved the use of a real minor engaging in sexually explicit conduct;

4. That such visual depiction is of a minor engaging in sexually explicit conduct; and

5. That the defendant knew that the individual in such visual depiction was a minor and knew that the visual depiction was of such minor engaged in sexually explicit conduct.

Sixth Circuit Pattern Jury Instruction No. 16.05, 2023 Edition.

The relevant statute for the second offense is Title 18, United States Code, Section 2252(A)(5)(b), which provides:

> "Any person who knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; shall be fined under this title or imprisoned not more than 10 years, or both . . . but, if any image of child pornography involved in the offense involved a prepubescent minor or a minor who had not attained 12 years of age, such person shall be fined under this title and imprisoned for not more than 20 years . . . "

18 U.S.C.§ 2252(A)(5)(b). To sustain its burden of proof for this crime, the United States must prove all of the following elements beyond a reasonable doubt:

1. Knowingly possessed or accessed with intent to view visual depiction;

2. Depicts actual minors engaged in sexually explicit conduct;

3. Aware of the sexually explicit nature and character of the material and that visual depictions are of minors engaged in sexually explicit conduct; and

4. Images had been mailed, or shipped, or transported in or affecting interstate or foreign commerce or produced using materials that had been mailed, or shipped or transported in or affecting interstate or foreign commerce.

Sixth Circuit Pattern Jury Instruction No. 16.08, 2023 Edition.

II. STATEMENT OF FACTS

In March of 2023, FBI agents ran investigative queries in a law enforcement service used to track Internet Protocol (IP) addresses suspected of trading Child Sexual Abuse Material (CSAM) via BitTorrent. ELOSHWAY'S IP address engaged in the receipt, possession, and distribution of files with matching MD5[1] values of known CSAM. This conduct occurred between February 13, 2022 through March 8, 2023. On March 27, 2023, ELOSHWAY'S IP address again was identified receiving and sharing parts of files known to be CSAM. During this time, ELOSHWAY'S IP address received or transmitted approximately 63,439 files, of which, approximately 9,541 files were determined to be severe files.[2] Of the files shared and downloaded, approximately 4,517 contained sadism and masochism.

On May 9, 2023, Agents executed search warrants on ELOSHWAY and his residence in Twinsburg, Ohio in the Northern District of Ohio, Eastern Division. Agents seized multiple devices from ELOSHWAY'S residence, specifically one black HP desktop computer. ELOSHWAY was advised of his rights and consented to an interview. ELOSHWAY stated the HP desktop contained child pornography. ELOSHWAY admitted he knew how BitTorrent

[1] MD5 is a nationally recognized file verification and authentication protocol used by the government and businesses to intercept and identify CSAM and to substantially compare like-files.

[2] Files of interest can be used by the law enforcement service to describe files that are child exploitative, age difficult, computer generated, or do not rise to the level of illegal, while severe files are described as CSAM.

worked and had been using it for 20 years. He stated he downloaded large batches of pornography from BitTorrent and those batches contained child pornography. He stated he would delete the child pornography that would be downloaded in batches. ELOSHWAY admitted the recent child pornography he downloaded had not been deleted and would be in his downloads folder on his computer.

ELOSHWYAY, via BitTorrent, distributed 62 files CSAM (five videos and 57 images) directly to law enforcement. The black HP desktop computer that ELOSHWAY admitted to storing child pornography on was analyzed and contained 7,182 unique files of CSAM (four videos and the remaining images).

III. STIPULATIONS

The government and the defendant have discussed the following stipulation and included it in the proposed jury instructions:

> The parties hereby agree and stipulate to the admission of Government Exhibit 1; and agree and stipulate that such exhibit accurately reflects information provided by representatives of Windstream.

Additional stipulations have been proposed but have not been agreed upon at this time. Defense proposed stipulating to the over 7,000 images of child pornography in this case and the government has declined this stipulation. See *United States v. Blank*, 701 F.3d 1084 (5th Cir. 2012) (the district court did not abuse its discretion by admitting two exhibits of child pornography discovered on defendant's computer, in his prosecution for transportation and possession of child pornography, notwithstanding that defendant offered to stipulate that material was child pornography, since prosecution was entitled to prove its case free from any defendant's option to stipulate evidence away).

IV. EVIDENTIARY QUESTIONS AND OTHER LEGAL ISSUES

A. EVIDENCE OF PEER-TO-PEER FILE SHARING AND BITTORRENT.

1. Peer-to-Peer File Sharing

Peer-to-peer file-sharing is a method of communication available to Internet users with free, publicly available software. Computers linked together through the Internet use this software to form a network which enables the sharing of digital files between users of that network. A user first obtains the peer-to-peer software, which can usually be downloaded from the Internet. In general, peer-to-peer software allows the user to set up files on a computer to be shared with others running compatible peer-to-peer software. A user obtains files by opening the software on their computer and conducting a search for files that are currently being shared on the network by other users.

BitTorrent is a very popular and publicly available peer-to-peer file sharing network. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network programs or "client" programs, examples of which include the uTorrent client program among others.

Files or sets of files are shared on the BitTorrent network via the use of "Torrents" (also ".torrents"). A Torrent is typically a small file that describes the file(s) to be shared. It is important to note that Torrent files do not contain the actual file(s) to be shared, but information about the file(s) to be shared. This information includes the "info hash," which is a SHA1 hash value1 of the set of data describing the file(s) referenced in the Torrent. This set of data contains the SHA1 hash value of each file piece in the Torrent, the file size(s), and the file name(s). This "infohash" uniquely identifies the Torrent file on the BitTorrent network.

To locate Torrent files of interest and download the files that they describe, a typical user will use keyword searches on Torrent-indexing websites, examples of which include

isohhunt.com and the piratebay.org. Torrent-indexing websites only host the Torrent files themselves and do not actually host the files described by Torrent files. A BitTorrent user seeking to download or share files through their client software on the BitTorrent network must voluntarily contact the BitTorrent index and voluntarily provide the BitTorrent index their IP address and the infohash of the data they wish to share. Once a Torrent file is located on the website that meets a user's keyword search criteria, the user will download the Torrent file to their computer. The BitTorrent network client program on the user's computer will then process that Torrent file to facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the Torrent file.

For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a Torrent-indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). Based on the results of the keyword search, the user would then select a Torrent of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the Torrent file. Utilizing BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the Torrent file and that these file(s) are available for sharing. The user can then download the file(s) directly from the computer(s) sharing them. Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file(s) with other users on the network. The downloaded file(s) are then stored in an area or folder previously designated by the user on the user's computer or on an external storage media. The downloaded file(s), including the Torrent file, will remain in that location until moved or deleted by the user.

Law enforcement can search the BitTorrent network to locate individuals sharing child pornography images which have been previously identified as such based on their SHA1 hash values. Law enforcement uses BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file(s) is downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

A peer-to-peer file transfer is assisted by reference to an IP address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer device during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers. The computer running the file sharing application, in this case a BitTorrent application, has an IP address assigned to it while it is on the internet. BitTorrent users can see the IP address of any computer system sharing files to them or receiving files from them. Investigators log the IP address which has sent them files or information regarding files being shared. Investigators can then search public records that are available on the internet to determine the internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the internet service provider via subpoena. Accordingly, in order to effectively use a peer-to-peer client software using the BitTorrent protocol, a user is making several pieces of information publicly available to all other users of the peer-to-peer network: (1) the IP address of their computer, which is necessary to share files between computers on the network (like a delivery address); (2) that the user's computer is employing a particular peer-to-peer client

program (here, a BitTorrent program); and (3) the content of any files a user is sharing via that peer-to-peer program, which the use—either by default, or by selection—has made available for other users to download through the peer-to-peer network.

2. The "Software Program" – Torrential Downpour

The BitTorrent software used in this case is a law enforcement sensitive computer software program called Torrential Downpour. Torrential Downpour was developed as a law enforcement investigative software tool in collaboration with computer programmers at the University of Massachusetts, Amherst, Department of Computer Science, Center for Forensics, specifically to investigate the online distribution of child pornography using the BitTorrent file-sharing protocol. Torrential Downpour is widely used by law enforcement at the federal, state, and local levels, and has resulted in hundreds, if not thousands, of search warrants, arrests, and convictions in child pornography cases. Torrential Downpour has been independently evaluated by a third party who found that the program is only able to conduct download from a single IP address (i.e., single source) and does not download from multiple IP addresses.

Torrential Downpour only accesses information and files available to the public via the peer-to-peer BitTorrent protocol. Torrential Downpour is configured to obtain downloads from a "single source" (i.e., one computer and one IP address), at a time. While publicly available Torrent software – for example, BitTorrent, which was located on the computer used by defendant – will download one file by drawing packets, or pieces, of the file from multiple users simultaneously to increase the download speed, Torrential Downpour is programmed to download a targeted file from only one user.

Torrential Downpour connects directly to a computer running BitTorrent software using the standard messaging protocols for that network, which are publicly available. The program

accesses the list of infohashes (.torrent files) selected by law enforcement related to known child pornography files. When a .torrent containing a suspected child pornography file(s) is identified, Torrential Downpour initiates a single-source download of that file(s) and creates a log of the download in real time. A law enforcement user of the Torrential Downpour software does not manually conduct downloads. Rather, the user sets certain restricting parameters and thereafter commences the software's operation. Torrential Downpour will then, on an automated basis, attempt to conduct downloads meeting the parameters that have been established by the user. A typical parameter set by law enforcement agents is a geographic restriction ensuring that the software only downloads from IP addresses within that law enforcement agency's jurisdiction.

Torrential Downpour is programmed such that it can only receive information and download files that are being shared using the peer-to-peer software running on the target computer. It cannot affirmatively upload or share any files or data with other network users Plainly stated, Torrential Downpour is an informational one-way street: it is programmed to receive but cannot share.

Torrential Downpour is also programmed to collect only publicly available information already shared by a BitTorrent user: for example, the file name and hash value of the shared pieces which make up the child pornography file(s); the computer's IP address; and the client software being used by the target to access the network. Torrential Downpour cannot access files that are not made available to the public through the file-sharing software. This is a function of not just Torrential Downpour, but of the BitTorrent protocol.

B. MENS REA AND KNOWLEDGE WHEN RECEIVING AND DISTRIBUTING CHILD PORNOGRAPHY

The first element of both counts one and two of the indictment require a mens rea of knowingly. When the government introduces testimony indicating: (1) defendant stated he knew

there was child pornography on his computer, (2) he stated that if there was any child pornography on his computer it was his, (3) he installed file sharing program on that computer, (4) he knew files in his file sharing folder would be shared with others, (5) file sharing folder contained child pornography, and (6) detective was able to access images of child pornography from defendant's computer via file sharing program, evidence is sufficient to support a conviction. *United States v. Frakes*, 402 Fed. Appx. 332, 2010 U.S. App. LEXIS 23472 (10th Cir. 2010). Knowledge can also be derived from defendant using terms associated with child pornography to search for and download images from peer-to-peer programs, especially in circumstances where defendant admits the images contained child pornography. *United States v. Haymond*, 672 F.3d 948, 2012 U.S. App. LEXIS 4652 (10th Cir. 2012).

Although distribution is not defined in the jury instructions, evidence consistent with the plain meaning of the word is sufficient. Specifically, evidence is sufficient to support a conviction for distribution under 18 USC § 2252(a)(2) when it shows that defendant maintained child pornography in a shared folder, knew that doing so would allow others to download it, and another person actually downloaded it. *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012).

Here, Eloshway has knowledge that he received, possessed, and distributed was child pornography. Eloshway admitted in an interview he knew there was child pornography on his computer. He stated the computer the child pornography was found on was his and he installed the file sharing program was the Bittorrent on that computer. Eloshway knew files in his file sharing folder would be shared with others as he stated he knew how BitTorrent worked and had been using it for 20 years. The file sharing folder contained child pornography, and finally, law enforcement was able to access images of child pornography from defendant's computer via file sharing program.

C. DEFENDANT'S SELF-SERVING EXCULPATORY STATEMENTS

It is well-settled that defendants cannot seek to introduce their own self-serving exculpatory statements. *United States v. McDaniel*, 398 F.3d 540, 545 (6th Cir. 2005) (citing *United States v. Wilkerson*, 84 F.3d 692, 696 (4th Cir. 1996), *cert. denied*, 522 U.S. 934 (1997)). Indeed, while the Federal Rules of Evidence allow the government to introduce inculpatory statements made by a defendant, the "Rules do not, however, provide an exception for self-serving, exculpatory statements made by a party which are being sought for admission by that same party." *Id.* Thus, while the government is permitted to introduce some or all of a defendant's statements against him as non-hearsay admissions of a party-opponent under Rule 801(d)(2), a defendant is not permitted to introduce his own statements under the same Rule. This rule applies equally to the evidence the defendant seeks to introduce in his own case as it does to the evidence he tries to elicit through the cross-examination of witnesses.

Eloshway spoke with law enforcement during the execution of the search warrant at his residence. Because the government may be introducing portions of the defendant's statements, it anticipates that Eloshway may try to elicit certain self-serving denials made during this conversation from the testifying law enforcement agent pursuant to Rule 106. In addition, or in the alternative, he may try to call another witness to elicit similar testimony. The "rule of completeness," however, does not override the prohibition from admitting self-serving, exculpatory statements. *Gallagher*, 57 Fed. Appx. at 628-29. The "completeness doctrine embodied in Rule 106 should not be used to make something admissible that would otherwise be excluded." *Id.*, *quoting Trepel v. Roadway Express, Inc.*, 194 F.3d 708, 718 (6th Cir. 1999); *see also United States v. Costner*, 684 F.2d 370, 373 (6th Cir. 1982). If the government were seeking to mislead the jury regarding the actual meaning of one of the defendant's admissions, the completeness doctrine might be implicated. That, however, is not the case here.

V. COURTROOM PROCEDURE

A. ANTICIPATED TRIAL LENGTH

The United States estimates that its presentation of evidence during trial will last approximately three days.

B. SEQUESTRATION OF WITNESSES & PRESENCE OF GOVERNMENT AGENT AT TRIAL

The United States respectfully requests that the Court issue a witness-sequestration order pursuant to Federal Rule of Evidence 615. The government designates FBI Special Agent Peter Mauro as its representative in this case to be present at counsel table throughout the trial. Agent Mauro's presence in the courtroom during trial is essential to the presentation of the government's case. *See* FED. R. EVID. 615(b) (specifically excluding from a sequestration order "an officer or employee of a party that is not a natural person, after being designated as the party's representative by its attorney"); FED. R. EVID. 615(c) (providing an additional exception for essential witnesses).

VI. CONCLUSION

The United States is prepared to submit additional briefing on any issue should the Court or circumstances require.

Respectfully submitted,

REBECCA C. LUTZKO
United States Attorney

By: /s/ Jennifer J. King
Jennifer J. King (OH: 0089375)
Assistant United States Attorney
801 West Superior Avenue, Suite 400
Cleveland, Ohio 44113
(216) 633-9421
Jennifer.King@usdoj.gov